UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/360,575	07/26/1999	SCOTT A. VANSTONE	67539/00230	4374

27871 7590 01/31/2006

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/360,575	VANSTONE, SCOTT A.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 9-19 are pending in this office action.

2. Applicant's arguments, filed November 17, 2005, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 9-14, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. (U.S. Patent No. 5,396,558) in view of Saito et al. (U.S. Patent No. 6,069,952).

With respect to Claim 9, Ishiguro et al. teaches a method of performing a transaction **in a communication system** between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment (abstract and col. 1, lines 1-15), said method comprising the steps of:

- **Upon initiation of said transaction by said first participant, said second participant sending a first message to said first participant, said first message including information pertaining to said second participant** (col. 2, lines 40-42);
- Said first participant verifying **said information pertaining to** said second participant to obtain assurance that said service will be provided upon **assuring said** payment (col. 2, lines 43-47);
- **Said first participant sending a second message to said second participant, said second message including information pertaining to said first participant** (col. 2, lines 48-51); and
- Said second participant verifying **said information pertaining to** said first participant to obtain assurance that payment will be secured upon provision of said service (col. 2, lines 52-56).

Ishiguro et al. does not teach **upon verification of said information pertaining to said first participant,** said second participant obtaining a digital signature for said first participant on said transaction **using said second message,** whereby said second participant may obtain payment from a third participant **using said digital signature**.

Saito et al. teaches **upon verification of said information pertaining to said first participant,** said second participant obtaining a digital signature for said first participant on said transaction **using said second message,** whereby said second

participant may obtain payment from a third participant **using said digital signature** (col. 39, line 58 through col. 42, line 58 of fig. 8, more specifically col. 42, lines 48-54 which shows the desirability of a digital signature).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Saito et al. within the system of Ishiguro et al because the digital signature protects the communication between the IC card and terminal from a replay attack, which is a common attack used to defraud unprotected businesses and customers. Also, the digital signature allows digital transactions to be performed that were only allowed by paper because of authentication and verification restraints (see col. 42, lines 55-58 of Saito et al.).

With respect to Claim 10, Ishiguro et al. in view of Saito et al. teaches the limitation of wherein said first participant is a holder of a card which performs cryptographic operations (see col. 2, lines 16-25 of Ishiguro et al.). The cryptographic operations are disclosed on col. 2, lines 26-61.

With respect to Claim 11, Ishiguro et al. in view of Saito et al. teaches the limitation of wherein said second participant is a terminal (see col. 2, lines 43-47 of Ishiguro et al.).

With respect to Claim 12, Ishiguro et al. in view of Saito et al. teaches the limitation of wherein said third participant is a financial institution (see fig. 8, ref. num 37/39/41 of Saito et al.).

With respect to Claim 13, Ishiguro et al. in view of Saito et al. teaches the limitation of **said information pertaining to said second participant included in said first message includes** details and credentials of said second participant (see col. 2, lines 48-51 of Ishiguro et al.); and **said first participant verifies said details and said credentials** (see col. 2, lines 52-56 of Ishiguro et al.).

With respect to Claim 14, Ishiguro et al. in view of Saito et al. teaches the limitation of **said information pertaining to said first participant included in said second message includes details and** credentials of said first participant (see col. 2, lines 40-42 of Ishiguro et al.); and **said second participant verifies said details and said credentials** (see col. 2, lines 43-47 of Ishiguro et al.).

With respect to Claim 18, Ishiguro et al. in view of Saito et al. teaches the limitation of wherein said credentials include a public key certificate (see col. 2, lines 52-56 of Ishiguro et al.). The presence of a public key and terminal identification number being used to verify validity of a digital signature requires the presence of a public key certificate.

With respect to Claim 19, Ishiguro et al. in view of Saito et al. teaches the limitation of wherein said challenge is a nonce (see fig. 10 and col. 16, lines 1-6 of Ishiguro et al.). A time stamp is used as a time variant parameter to prevent against replay attacks.

Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. (USPN '558) in view of Saito et al. (USPN '952) in further view of Chaum (U.S. Patent No. 5,276,736).

With respect to Claim 15, all the limitation above are met by the combination of Ishiguro et al. in view of Saito et al. except the limitation disclosed below.

Chaum meets the limitation of said second participant generating a response to said challenge (col. 3, lines 57-60); and said second participant sending a third message including said response to said first participant (col. 3, lines 57-60); and said first participant verifying said response (col. 3, lines 52-55 and 57-62); and said first participant sending a fourth message to said second participant such that said digital signature is provided by said second message and said fourth message (col. 4, lines 20-27, 57-60). The message being signed reflects a digital signature being appended to the message being sent.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chaum within the combination of Ishiguro et al and Saito et al. because verification of the challenge prevents an outside attacker from using a replay attack to gain access to the system. The challenge is unique and once verified, provides a greater guarantee that the transaction is in fact legitimate.

With respect to Claim 16, the combination of Ishiguro et al. in view of Saito et al./Chaum teach said second participant verifying information in said fourth message (see col. 4, lines 20-27 of Chaum); and said second participant completing said transaction by providing said service (see col. 4, lines 44-47 and 57-60 of Chaum); and said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain **said** payment (see col. 4, lines 35-45 of Chaum).

With respect to Claim 17, the combination of Ishiguro et al. in view of Saito et al./Chaum teach said third participant verifying said subset (see col. 4, lines 37-43 of Chaum); and said third participant providing **said** payment to said second participant (see col. 4, lines 44-47 of Chaum).

Response to Arguments

5. Applicant amends claims 9 and 13-17.

6. Applicant argues:

a. The combination of Ishiguro et al. and Saito et al. do not teach upon verification of the first two participants, the second participant obtaining a digital signature from the first participant that is used to obtain a payment from a third participant. Applicant argues that Ishiguro et al. does not even contain a third party, therefore, the combination with Saito et al. (which includes a third party) would not arrive at the claimed invention and there is no motivation to combine (page 6 through page 7).

b. The dependent claims are allowable based on their dependency on the independent claim (page 7, last two paragraphs).

Regarding argument (a), examiner disagrees with applicant. First off, there exists a third party in Ishiguro et al. The third party is the management center. Ishiguro et al. teaches (at col. 13, line 21 through col. 15, line 6) that the IC card exchanges messages with the IC card terminal and then periodically (once a day) the IC card terminal will interact with the management center to update values for the day corresponding to a specific IC card. The IC card is identified in the management center by the IC card terminal providing information pertaining to the IC card to the management center (such as the IC card identification number). In order for the IC card terminal to be able to identify the IC card to the management center (similar to a liaison or proxy providing information to one person on behalf of another person), the received information from the IC card is then forwarded to the management center. This combined with Saito et al. teaches a three party exchange (bank, customer, and retail

shop) where the customer is the first party and the shop is the second party. The second party (retail shop) does not need to contact the third party (bank) with every transaction. The second party (retail shop) can simply contact the third party (bank) once a day, possibly at the end of the day. This eliminates the need for the second party (retail shop) to contact the third party (bank) every single transaction, which costs the second party (retail shop) money (see col. 2, lines 18-25 of Ishiguro et al.).

Regarding argument (b), examiner disagrees with applicant. Based on the response by examiner for argument (a), above, the dependent claims stand as rejected.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

Primary Examiner
AU2131
1/25/06